Risk Management Framework References

Gary E. McGraw, Cigital, Inc. [vita[3]]

2005-09-21

Publications relevant to technology risk management.

The following standards documents and government publications are directly relevant to technology risk management. A number of the five stages described in the RMF can be enhanced with various parts of the processes described in these documents. Of particular relevance are the charts and tables defined by NIST[4].

- *IEC 61508; Parts 3, 6 and 7; Version 4.0 (1997) Functional Safety and IEC 61508 — A Basic Guide* can be found at http://www.iee.org/oncomms/pn/functionalsafety/HLD.pdf.
- *NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.* The NIST publications can be found at http://csrc.nist.gov/publications/nistpubs/.
- *NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Section 2.4, Categories of Information Systems.* The NIST publications can be found at http://csrc.nist.gov/publications/nistpubs/.
- *NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.* The NIST publications can be found at http://csrc.nist.gov/publications/nistpubs/.

In addition to these standards, a number of other references are useful.

References

[Anderson 01]	Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York, NY: John Wiley and Sons, 2001.
[Cavusoglu 02]	Cavusoglu, H.; Mishra, B.; & Raghunathan, S. *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers*. Dallas, TX: University of Texas at Dallas, 2002.
[Hoglund 04]	Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code.*. Boston, MA: Addison-Wesley, 2004.
[Howard 01]	Howard, M. & LeBlanc, D. *Writing Secure Code*.

3. daisy:198 (McGraw, Gary)

4. The NIST charts and tables cover topics such as security controls (800-53), information systems vulnerabilities and mission risk, a security certification and accreditation processes for a large and complex system (800-37), integrating risk management into the SDLC, risk assessment methodology, human threats (source, motivation, and actions), vulnerability threat pairs, risk level and scale and necessary actions, risk mitigation action points, risk mitigation and methodology flow chart, technical security controls, implemented controls and residual risk, sample safeguard implementation plan summary (800-30).

Redmond, WA: Microsoft, 2001.

[Howard 03c] Howard, M. & Lipner, S. "Inside the Windows Security Push." *IEEE Security & Privacy* 1, 1 (Jan.-Feb. 2003): 57-61.

[McGraw 03d] McGraw, G. "From the Ground Up: The DIMACS Software Security Workshop." *IEEE Security & Privacy* 1, 2 (March-April 2003): 59-66.

[McGraw 04] McGraw, G. "Software Security." *IEEE Security & Privacy* 2, 2 (March-April 2004): 80-83.

[Saltzer 75] Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." 1278-1308. *Proceedings of the IEEE 63.* 9. IEEE. September 1975.

[Verdon 04] Verdon, Denis & McGraw, Gary. ”Risk Analysis in Software Design.” *IEEE Security & Privacy* 2, 4 (July-Aug. 2004): 79-84.

[Viega 00] Viega, J.; Bloch, J.; Kohno, T.; & McGraw, G.. "ITS4: A Static Vulnerability Scanner for C and C++ Code." *Proceedings of Annual Computer Security Applications Conference*. New Orleans, LA, December 11-15, 2000. http://www.acsac.org/2000/papers/78.pdf.

[Viega 02] Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley, 2002.

[Wagner 00] Wagner, D.; Foster, J.; Brewer, E.; & Aiken, A. "A First Step Towards Automated Detection of Buffer Over-run Vulnerabilities." *Proceedings of the Year 2000 Network and Distributed System Security Symposium* (NDSS). San Diego, CA, February 3-4, 2000. http://www.isoc.org/isoc/conferences/ndss/2000/.

[Walsh 03] Walsh, L. "Trustworthy Yet?" *Information Security Magazine*, February 2003. http://infosecuritymag.techtarget.com/2003/feb/cover.shtml.

[Wing 03] Wing, J. "A Call to Action: Look Beyond the Horizon." *IEEE Security & Privacy* 1, 6 (Nov.-Dec. 2003): 62-67.

Cigital, Inc. Copyright

Fields

Name	Value
Copyright Holder	Cigital, Inc.

Fields

Name	Value
is-content-area-overview	false
Content Areas	Best Practices/Risk Management
SDLC Relevance	Requirements
Workflow State	Publishable

1. mailto:copyright@cigital.com